

NR:VTN  
F. #2018R01745

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF  
ONE LG MOBILE TELEPHONE  
BEARING MEID NUMBER  
35963409585903 AND ONE MOTOROLA  
MOBILE TELEPHONE BEARING MEID  
NUMBER 99000572146942

APPLICATION FOR A SEARCH  
WARRANT FOR ELECTRONIC  
DEVICES.

Case No. 19-MJ-340

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Joshua E. Croft, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of electronic devices, described below and in Attachment A, that are currently in law enforcement's possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been employed as a Special Agent with Homeland Security Investigations ("HSI"), within the Department of Homeland Security, since 2016. I am currently assigned to the Child Exploitation Investigations Unit. During my tenure with HSI, I have participated in investigations targeting individuals involved in the receipt, distribution and possession of child pornography and have conducted physical and electronic surveillance, executed search warrants, reviewed and analyzed electronic devices, and

interviewed witnesses. As part of my employment with HSI, I successfully completed the Federal Law Enforcement Training Center's Criminal Investigator Training Program and Immigration and Customs Enforcement Special Agent Training, both of which included instruction with respect to the application for, and execution of, search and arrest warrants, as well as the application for criminal complaints and other legal processes.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of criminal statutes relating to the sexual exploitation of children, specifically Title 18, United States Code, Sections 2251, 2252 and 2252A (the "Subject Offenses") have been committed by ANDRE WILBURN. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband and fruits of these crimes, as further described in Attachment B.

#### **IDENTIFICATION OF THE DEVICES TO BE EXAMINED**

5. The property to be searched is one LG mobile telephone bearing MEID number 35963409585903 and one Motorola mobile telephone bearing MEID number 99000572146942, hereinafter the "Devices." The Devices are currently in the custody of HSI within the Eastern District of New York.

**PROBABLE CAUSE**

6. On or about and between August 21, 2018 and August 27, 2018, special agents from the Child Exploitation Investigations Unit of HSI conducted a forensic search of data received from Google, Inc., that is associated with ANDRE WILBURN and his email account of dre@linkrange.com (the “Dre Google Drive”). Google Drive is a file storage and synchronization service developed by Google. It allows users to store files on their servers, synchronize files across devices, and share files. The search of the Dre Google Drive was conducted pursuant to a search and seizure warrant authorized by the Honorable Lois Bloom, Magistrate Judge for the Eastern District of New York, on August 14, 2018. (See Dkt. No. 18-MJ-748).

7. During the forensic search, law enforcement authorities identified approximately 105 images of child pornography (the “CP Images”) on the Dre Google Drive. Based on a review of the metadata pertaining to the CP Images, law enforcement authorities believe that the CP Images were stored on the Dre Google Drive between approximately November 2016 through July 25, 2018.

8. Approximately 15 of the CP Images show a man’s penis orally penetrating a female toddler, who appears to be approximately two years old. Three of those CP images are described as follows.

- a. 20180113\_202409.jpg shows a toddler, approximately two years old, seated on a bed with an erect adult male penis inserted in the child’s mouth.
- b. 20161106\_174547.jpg shows a toddler, approximately two years old, standing against a wall while an adult male holds his erect penis in front of the child’s face.

- c. 20161106\_174556.jpg shows a toddler, approximately two years old, standing against a wall with an erect adult male's penis inserted in the child's mouth.

9. Law enforcement authorities determined that ANDRE WILBURN resided in an apartment owned and managed by the New York City Housing Authority in New York, New York ("WILBURN's Apartment"). On or about August 29, 2018, the Honorable Barbara C. Moses, Magistrate Judge for the Southern District of New York, granted an application for a warrant to search WILBURN's Apartment for evidence or instrumentalities of violations of Title 18, United States Code Sections 2251, 2252, and 2252A. (See S.D.N.Y. Dkt. No. 18-MAG-7476). On or about September 6, 2018, HSI conducted a search of WILBURN's Apartment pursuant to the warrant.

10. Based in part on evidence found inside WILBURN's Apartment, I believe that the male in the images described in the paragraph 8 above is ANDRE WILBURN for the reasons described below:

- a. The metadata, specifically the EXIF data<sup>1</sup>, pertaining to the CP Images depicting the toddler indicate that they were all taken with a Samsung Galaxy SM-G935F mobile telephone. A review of the Dre Google Drive shows that a Samsung Galaxy SM-G935F mobile telephone accessed the Dre Google Drive on or about February 26, 2018. On or about September 6, 2018, law enforcement authorities recovered an empty mobile telephone box for a Samsung Galaxy SM-G935F inside WILBURN's bedroom in WILBURN's Apartment.

---

<sup>1</sup> EXIF stands for Exchangeable Image File and its associated data can be stored to a variety of image file formats. EXIF data reveals information about the camera and settings that were used to take the photos, such as the date and time, focal length, shutter speed, or white balance settings.

- b. Based on a comparison of the background visible in the CP Images depicting the toddler to the physical appearance of WILBURN's Apartment, law enforcement authorities believe that the CP Images involving the toddler were taken inside WILBURN's bedroom. Specifically, law enforcement authorities observed a bedspread on WILBURN's bed that appears identical to the bedspread visible in many of the CP Images involving the toddler. Law enforcement authorities also recovered a space-heater from a closet inside WILBURN's Apartment which is visible in many of the CP Images depicting the toddler.
- c. Based on a forensic review of the Dre Google Drive for evidence of user attribution, which includes email messages, text messages, images, videos, references to social media accounts and other content of the Dre Google Drive, law enforcement authorities believe that the Dre Google Drive was exclusively used by WILBURN.

11. During the search of WILBURN's Apartment, law enforcement agents seized several electronic devices and conducted a forensic examination of those devices as authorized by the warrant. During my examination of those devices, I identified thousands of images of child pornography on multiple devices. Those findings are summarized as follows:

- a. On one LG LS740 Volt mobile telephone bearing serial number 411CYJZA0784236, I identified approximately 223 images of child pornography depicting minors between the approximate ages of 2 and 14, all of which appeared to have been downloaded from the internet.
- b. On one Toshiba hard drive bearing serial number 43ILPBSMTTB2, I identified approximately 1735 images of child pornography depicting minors between the approximate ages of 2 and 12, all of which appeared to have been downloaded from the internet.
- c. On one Seagate hard drive bearing the serial number 9QG9JPBH, I identified approximately 69,034 images of child pornography depicting minors as young as infants and other minors up through the approximate age of 14, all of which appeared to have been downloaded from the internet. Approximately 227 of those images depict minors being

subjected to bondage and bestiality.

- d. On one Toshiba hard drive bearing the serial number 92DGP39ZTTZ2, I identified approximately 44,830 images of child pornography depicting minors as young as infants and other minors up through the approximate age of 14, all of which appeared to have been downloaded from the internet. Approximately 130 of those images depict minors being subjected to bondage and bestiality.

12. On or about September 7, 2018, the Honorable Vera M. Scanlon Judge, Magistrate Judge for the Eastern District of New York, granted an application for a warrant to arrest ANDRE WILBURN for violations of Title 18, United States Code, Sections 2251(a) and 2252(a)(2).

13. On or about January 7, 2019, law enforcement officers spoke with a relative (the "Relative") of one of the victims of ANDRE WILBURN's charged offenses. The Relative stated, in substance, that WILBURN had contacted him/her through an Instagram account used by WILBURN and asked the Relative to download an encrypted messaging application. WILBURN began communicating with the Relative on the encrypted messaging application.

14. Thereafter, law enforcement officers, with the consent of the Relative, began monitoring the communications between ANDRE WILBURN and the Relative, including video communications where WILBURN appeared on the screen. Law enforcement agents recognized WILBURN as the individual who was communicating with the Relative. Based on a text message sent by WILBURN, agents determined that he was located in San Diego, California.

15. On or about January 14, 2019, law enforcement agents monitored an online video chat session between the Relative and WILBURN, who was using a mobile telephone. During the video chat, the Relative asked WILBURN if he had obtained a new telephone. WILBURN responded that the mobile telephone he was using was “one of the random phones I grabbed out of my car before I came over here.” The mobile telephone that WILBURN was using during the video chat appears to be the one of the Devices described herein, specifically the Motorola mobile telephone, based upon the color, size, shape and location of the camera lens of the mobile telephone law enforcement authorities observed during the video chat.

16. On or about January 15, 2019, law enforcement officers arrested WILBURN in San Diego, California. Special Agent Johnathan Willis of HSI San Diego recovered the Devices from WILBURN.

17. On or about February 28, 2019, an indictment was filed against WILBURN charging him with one count of sexual exploitation of a child and one count of possession of child pornography, in violation of Title 18, United States Code, Sections 2251(a) and 2252(a).

18. Based upon my training and experience as a special agent, I believe that the Devices are likely to contain evidence, instrumentalities, contraband and fruits of the Subject Offenses for the following reasons.

- a. WILBURN has previously utilized multiple devices, including mobile telephones to exploit children. More specifically, to date law enforcement agents have identified two different mobile telephones belonging to WILBURN that were used by WILBURN to produce, receive and possess images of child pornography. (See paragraphs 10(a) and 11(a) above).

- b. Based on my training and experience in conducting investigations relating to child exploitation, I am aware that individuals who receive and possess child pornography are aware of the criminality of their conduct and thus take steps to hide that conduct. Among other things, I am aware that such individuals often use multiple devices to possess and receive illegal images in an attempt to hide their identities and avoid leaving a clear digital “footprint” of their conduct.
- c. Based on my training and experience in conducting investigations relating to child exploitation I am also aware that individuals who produce, receive and possess images of child pornography often demonstrate compulsive tendencies and endeavor to obtain a large volume of illegal images. I am further aware, from past investigations that a standard condition of pretrial release for many defendants charged with one or more of the Subject Offenses is to have their electronic devices monitored by Pretrial Services to ensure that they do not continue to engage in similar conduct. The high volume of child pornography found to date on different electronic devices owned and used by WILBURN (see paragraph 11 above) make it more likely that the Devices contain evidence of the Subject Offenses.
- d. As law enforcement agents seized the electronic devices found inside WILBURN’s Apartment on September 6, 2018, during the execution of a search warrant, WILBURN needed to obtain additional means by which to access the internet, his email and other electronically stored information, including data on the Dre Google Drive. For example, as set forth above, there is probable cause to believe that WILBURN used one of the Devices to communicate with the Relative using Instagram and an encrypted messaging application. Records of such communications, particularly the ones that were made before the Relative was contacted by law enforcement authorities and thus were not consensually monitored, are likely to be on at least one of the Devices and reflect WILBURN’s knowledge of and access to one of the victims of WILBURN’s charged offenses

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

19. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.



20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on

the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to view or download images of child pornography over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

**CONCLUSION**

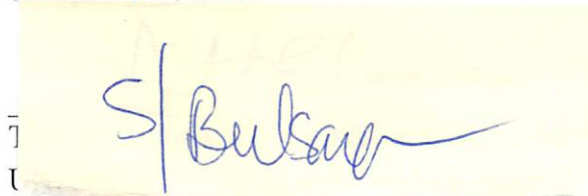
23. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B. Because the Devices are already in the custody of law enforcement, reasonable cause exists to permit the execution of the requested search at any time in the day or night.

Respectfully submitted,



Joshua E. Croft  
Special Agent  
Homeland Security Investigations

Subscribed and sworn to before me  
on April 12, 2019:



EASTERN DISTRICT OF NEW YORK

**ATTACHMENT A**

The property to be searched is one LG mobile telephone bearing MEID number 35963409585903 and one Motorola mobile telephone bearing MEID number 99000572146942, hereinafter the “Devices.” The Devices are currently in the custody of Homeland Security Investigations within the Eastern District of New York.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. Sections 2251, 2252 and 2252A and involve ANDRE WILBURN, including the following:

1. images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the production, possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation 18 U.S.C. §§ 2252 and 2252A, in any form wherever they may be stored or found;
2. motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
3. records and information pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct;
4. records and information concerning any Internet accounts used to possess, receive or distribute child pornography;
5. evidence of who used, owned, or controlled the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;
6. evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the

presence or absence of security software designed to detect malicious software; and evidence of the lack of such malicious software;

7. evidence of the attachment to the Devices of other storage devices or similar containers for electronic evidence;

8. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Devices;

9. evidence of the times the Devices were used;

10. passwords, encryption keys, and other access devices that may be necessary to access the Devices;

11. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the Devices; and

12. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, and any photographic form.